대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0032083
Application Number

출 원 년 월 일 : 2003년 05월 20일
Date of Application MAY 20, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 12 월 19 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0004
【제출일자】	2003.05.20
【발명의 명칭】	데이터 복제방지 장치와 시스템 및 복제방지 방법
【발명의 영문명칭】	Apparatus and System for Data Copy Protection and Method therefor
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	김동진
【대리인코드】	9-1999-000041-4
【포괄위임등록번호】	2002-007585-8
【발명자】	
【성명의 국문표기】	최양림
【성명의 영문표기】	CHOI,Yang Lim
【주민등록번호】	710120-1830615
【우편번호】	463-060
【주소】	경기도 성남시 분당구 이매동 124 한신아파트 210-1509
【국적】	KR
【발명자】	
【성명의 국문표기】	최윤호
【성명의 영문표기】	CHOI,Yun Ho
【주민등록번호】	730121-1480318
【우편번호】	138-912
【주소】	서울특별시 송파구 잠실2동 주공아파트 259-407
【국적】	KR
【발명자】	
【성명의 국문표기】	김윤상
【성명의 영문표기】	KIM,Yun Sang
【주민등록번호】	681007-1066619

【우편번호】	441-837
【주소】	경기도 수원시 권선구 권선동 1265번지 유원.보성아파트 605동 1205 호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 김동진 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	0 면 0 원
【우선권주장료】	0 건 0 원
【심사청구료】	16 항 621,000 원
【합계】	650,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 데이터 복제방지 장치와 시스템 및 복제방지 방법에 관한 발명으로서, 데이터의 복제방지를 위한 제어정보를 설정하고, 상기 설정된 제어정보에 따른 각각의 제어모드에 따라 상기 데이터를 암호화하고, 상기 암호화된 데이터를 전송하는 전송장치와 상기 전송된 데이터를 수신하여 상기 제어정보를 추출하고, 상기 추출된 제어정보에 따른 각각의 제어모드에 대응하여 데이터를 해독하는 수신장치와 상기 전송장치와 수신장치를 포함하는 데이터 복제방지를 위한 시스템을 특징으로 한다.

【대표도】

도 3

【색인어】

데이터 복제, 카피제어정보(CCI), 데이터 암호와 해독

【명세서】

【발명의 명칭】

데이터 복제방지 장치와 시스템 및 복제방지 방법{Apparatus and System for Data Copy Protection and Method therefor}

【도면의 간단한 설명】

도 1은 카피제어정보(Copy Control Information;CCI) 코드에 따른 AV스트림 데이터의 암호화 상태를 나타내는 예시도.

도 2는 본 발명에 따른 카피제어정보 코드에 따른 AV스트림 데이터의 암호화 상태 및 암호/해독 모드를 나타내는 예시도.

도 3은 본 발명에 따른 데이터 암호화를 위한 장치의 구성을 나타내는 예시도.

도 4는 본 발명에 따른 데이터 해독을 위한 장치의 구성을 나타내는 예시도.

도 5a는 본 발명에 따른 데이터 암호화 과정을 나타내는 일실시예 처리 흐름도.

도 5b는 본 발명에 따른 데이터 해독 과정을 나타내는 일실시예 처리 흐름도.

도 6은 본 발명에 따른 3가지 유형의 2-bit 값을 내장하고 있는 데이터 해독을 위한 장치의 구성을 나타내는 예시도.

도 7은 본 발명에 따른 3종류의 DES 암호를 이용한 데이터 해독을 위한 장치의 구성을 나타내는 예시도.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<9> 본 발명은 데이터 복제방지 장치와 시스템 및 복제방지 방법에 관한 것으로, 보다 상세하게는 데이터의 복제방지를 위한 제어정보에 따른 각각의 제어모드에 따라 암호화하는 방법을 다르게 함으로써 제3자에 의한 데이터의 불법복제를 방지하는 방법에 관한 것이다.

<10> 디지털 신호처리 기술이 발전함에 따라 다양한 종류의 디지털 기록 장치 및 기록매체가 널리 보급되고 있다. 그러나, 이러한 장치 및 기록매체에 포함된 디지털 데이터는 반복적인 재생과 복사가 가능하므로 복사가 위법으로 행해진 기록매체가 시장에 유통하게 되면, 음악, 영화 등 각종 컨텐츠의 저작권자 또는 정당한 판매권자 등의 이익이 침해될 우려가 있다. 최근에는 이러한 디지털 데이터의 부정한 복사를 막기 위해 여러 가지 방법이 도입되고 있는데, 그 중, 카피제어정보(Copy Control Information; 이하 'CCI'라고 한다)를 이용하는 방법이 있다.

<11> 일반적으로 컨텐츠는 각각 미리 컨텐츠 제공자에 의해 어떠한 조건으로 복제가 가능한지 지정되어 있다. 그래서, 네트워크 접속에 있어서도 그 지정된 조건을 정확하게 상대의 기기에 전할 필요성이 있어, 5개 기업의 공동 제안으로서의 5C DTCP (Digital Transmission Content Protection) 시스템으로서는 상기 CCI를 이용하여 해결하고 있다. 이러한 CCI정보는 2비트의 코드로 표시되며, 4가지 유형의 모드를 설정하는 것이 가능하다. CCI 정보의 구성을 좀더 구체적으로 살펴보면, 도 1에서 도시한 바와 같은데, '00'은 어떠한 인증이나 암호화가 필요없고 암호화를 수행하지 않기 때문에 AV스트림은 자유롭게 복사가 가능한 카피 프리(copy free)를 나타내고, '01'은 자유롭게 복사할 수 있으나 암호화가 되어 있으므로 암호화된 AV스트림을 해

독할 수 있는 장치라면 자유롭게 카피할 수 있는 'copy free but encrypted'를 나타내고, '10'은 한번만 복사가 가능하고 복사한 후부터는 복사가 금지되는 'copy one generation'을 나타내고, '11'은 절대로 복사가 금지되는 'no more copy or copy never'를 나타낸다.

<12> 그런데, AV 스트림내에 기록되어 있는 CCI 코드의 유형이 다르더라도, 암호 상태(status)가 "암호화" 라는 상태를 나타내면 컨텐츠는 동일한 암호화 방법을 사용해서 기록되어 있으며 동일한 해독방법이 적용되므로, CCI 정보를 불법으로 변경한다면 복사가 허용되지 않는 contents, 즉 "no more copy or copy never" 의 정보를 갖고 있는 컨텐츠의 불법복제가 가능하다. 예를 들어서 "copy one generation" or "no more copy or copy never" 의 CCI 정보를 "copy free but encrypted" 모드로 변경한다면, 동일한 암호/해독 방법이 적용되어 있으므로 컨텐츠가 쉽게 해독되어 무한정의 불법복제가 가능하게 된다. 또한, "no more copy or copy never" 의 CCI 정보가 "copy one generation" 의 CCI 정보로 불법 변경되는 경우도 마찬가지로 한번의 복사가 가능하게 된다.

<13> 또한 기존의 기술에서는 컨텐츠의 중요도를 떠나 암호 상태(Status)가 "암호화" 라는 상태를 나타내면 보안 등급(security level)에 관계없이 동일한 암호/해독의 동작이 이루어지므로, 실질적으로 보안 등급의 의미를 상실하게 된다.

<14> 또 다른 문제점으로 컴플라이언스 룰(compliance rule)과 관련하여 살펴볼 수 있다. 기존기술은 시스템 구현에 있어서 CCI 정보값이 유효한지 아닌지를 검사하는 컴플라이언스 룰(compliance rule)이 존재하지 않는다. 즉, 구현된 하드웨어 또는 소프트웨어 시스템에서 입력 데이터 값과 기록되어 있는 CCI 값을 비교하는 강요사항이 없다. 이것은 CCI 정보의 불법변경에 대하여 하드웨어 또는 소프트웨어 시스템 내에서는 방지할 수 없다는 것을 나타낸다.

<15> 따라서, 본 발명에서는 상기와 같은 문제점을 개선하고자 한다.

【발명이 이루고자 하는 기술적 과제】

<16> 본 발명은 상기한 문제점을 개선하기 위해 안출된 것으로, 본 발명에서는 데이터의 복제방지를 위한 제어정보에 따른 각각의 제어모드에 따라 데이터의 암호화 및 해독방법을 다르게 함으로써 복제방지 제어정보의 불법 변경으로 인한 컨텐츠의 해독 및 불법복제를 효과적으로 방지하고 컨텐츠의 중요도에 따른 암호,해독방법을 달리함으로써 (예를 들면 11 : high, 10 : medium, 01 : low) 컨텐츠의 보안성을 더욱 유지할 수 있는 방법을 제안한다.

【발명의 구성 및 작용】

<17> 상기 목적을 달성하기 위하여, 본 발명에 따른 데이터 복제방지 장치는 데이터의 복제방지를 위한 제어정보를 설정하는 제어정보 설정부, 상기 설정된 제어정보에 따른 각각의 제어모드에 따라 상기 데이터를 암호화하는 데이터 암호화부,상기 데이터 암호화부에서 제공하는 데이터를 전송하는 데이터 전송부를 포함하는 데이터 복제방지를 위한 전송장치와, 데이터의 복제방지를 위한 제어정보를 포함하고, 상기 제어정보에 따른 각각의 제어모드에 대응하여 암호화된 데이터를 수신하는 데이터 수신부, 상기 수신된 데이터로부터 상기 제어정보를 추출하는 제어정보 추출부, 상기 추출된 제어정보에 따른 각각의 제어모드에 대응하여 데이터를 해독하는 데이터 해독부를 포함하는 데이터 복제방지를 위한 수신장치를 포함한다.

<18> 또한, 본 발명에 따른 데이터 복제방지 시스템은 상기 전송장치와 수신장치를 포함한다.

<19> 또한, 본 발명에 따른 데이터 복제방지 방법은 복제방지를 위한 제어정보를 설정하고, 상기 설정된 제어정보에 따른 각각의 제어모드에 대응하여 데이터를 암호화하여 전송하는 제1단계, 상기 전송된 데이터를 수신하고, 상기 수신한 데이터로부터 상기 제어정보를 추출하는 제2단계,

상기 추출된 제어정보에 따른 각각의 제어모드에 대응하여 데이터를 해독하는 제3단계를 포함한다.

<20> 이하, 첨부된 도면을 참조하여 본 발명의 일실시예에 따른 데이터 복제방지 장치와 시스템 및 데이터 복제방지 방법을 설명하면 다음과 같다.

<21> 한편, 본 발명에 있어서 데이터는 편의상 AV스트림 데이터를 포함하고 있는 컨텐츠를 예로 하고, 복제방지를 위한 제어정보는 CCI를 예로 설명하기로 한다.

<22> 도 2는 본 발명에 따른 카피제어정보 코드에 따른 AV스트림 데이터의 암호화 상태 및 암호/해독 모드를 나타내는 예시도로서, CCI 코드의 변경으로 인한 불법복제를 방지하기 위해 컨텐츠의 암호화/해독 모드를 달리 설정한다. 즉, '01'의 경우는 'copy free but encrypted'를 나타내는 모드 1을 나타내고, '10'의 경우는 'copy one generation'을 나타내는 모드 2를 나타내고, '11'의 경우는 'no more copy or copy never'를 나타내는 모드 3을 나타낸다.

<23> 도 3은 본 발명에 따른 데이터 암호화를 위한 장치의 구성을 나타내는 예시도로서, 데이터 복제방지를 위한 전송장치(300)는 CCI코드 결정부(320), 데이터를 암호화하는 암호화모듈(330), 암호화된 AV스트림 또는 암호화되지 않은 AV스트림을 전송하는 AV스트림 전송부(340)를 포함한다. 상기 CCI코드 결정부(320)에서는 AV스트림에 어떠한 CCI코드를 추가하여 컨텐츠(310)를 암호화할 것인지를 결정한다. 그 결정된 값이 "copy free" 인 "00" 의 값을 가지면 암호화모듈(330)을 거치지 않고 암호화되지 않은 상태로 AV스트림 전송부(340)을 통하여 임의의 기록매체에 저장되거나 전송매체를 통하여 전송된다. 반면에 "copy free but encrypted (01), copy one generation (10), no more copy or copy never (11)" 인 경우에는 암호화모듈(330)에서 서로 다른 암호화 모드에 의해서 컨텐츠가 암호화되어 AV스트림 전송부(340)를 통해 임의의 기록매체에 저장되거나 전송매체를 통하여 전송된다. 즉,

"01" 인 경우는 모드 1, "10" 인 경우는 모드 2, "11" 인 경우는 모드 3 으로 각각 다르게 암호화되어(331,332,333) 암호화모듈(330)이 동작하게 된다.

<24> 도 4는 본 발명에 따른 데이터 해독을 위한 장치의 구성을 나타내는 예시도로서, 데이터 복제 방지를 위한 수신장치(400)는 CCI코드 검사부(420), 데이터를 해독하는 암해독모듈(430), 해독된 AV스트림 또는 해독하지 않은 AV스트림을 출력하는 AV스트림 출력부(340)를 포함한다. CCI코드 검사부(420)는 수신한 AV스트림(410)이 어떠한 CCI코드를 갖고 있는지 검사한다. 만일, CCI코드가 "copy free"인 "00"을 나타내면, 해독모듈(430)을 거치지 않고 AV스트림 출력부(440)를 통해 AV스트림이 출력된다. 반면에 "copy free but encrypted (01), copy one generation (10), no more copy or copy never (11)" 인 경우에는 서로 다른 해독모듈(430)에 의해서 AV스트림이 해독되어 AV스트림 출력부(440)를 통해 출력된다. 즉"01" 인 경우는 모드 1 해독모듈(431)을 통해, "10" 인 경우는 모드 2 해독모듈(432)을 통해, "11" 인 경우는 모드 3 해독모듈(433)을 통해 각각 해독되어 AV스트림 출력부(440)를 통해 출력된다.

<25> 도 5a는 본 발명에 따른 데이터 암호화 과정을 나타내는 일실시예 처리 흐름도로서, 그 과정을 살펴보면, 컨텐츠를 수신하여 컨텐츠 정보에 따른 CCI코드를 결정하고(S510), 상기 결정된 CCI코드를 검사하여(S512) CCI코드값이 '00'이면 암호화되지 않고 곧바로 광기록매체와 같은 미디어에 기록한다(S518). 만일 CCI코드값이 '00'이 아니라면, CCI코드값에 대응하는 암호 모드를 선택한다(S514). 즉, '01'인 경우에는 모드 1, '10'인 경우에는 모드 2, '11'인 경우에는 모드 3이 된다. 상기 암호 모드가 선택되면, 상기 암호 모드에 대응하는 암호화를 수행하고(S516), 암호화된 컨텐츠를 광기록매체와 같은 미디어에 기록한다(S518). 이 때, 미디어에 기록하는 대신 유,무선 전송매체를 통해 암호화된 컨텐츠를 해독하는 장치로 전송할 수도 있다.

<26> 도 5b는 본 발명에 따른 데이터 해독 과정을 나타내는 일실시예 처리 흐름도로서, 그 과정을 살펴보면, 암호화된 데이터를 해독하는 장치(device)에 데이터가 기록된 광기록매체와 같은 미디어를 삽입한다(S550). 이 때, 상기 미디어 대신 유,무선 전송매체를 통해 데이터를 수신할 수도 있다. 상기 미디어 또는 전송매체를 통하여 수신한 데이터로부터 CCI를 검사하여(S552) 만일 CCI코드값이 '00'이면, 수신한 컨텐츠를 해독하지 않고 곧바로 AV스트림을 출력한다. 만일, CCI코드값이 '00'이 아니라면, CCI코드값에 대응하는 암호 모드를 선택한다(S554). 즉, '01'인 경우에는 모드 1, '10'인 경우에는 모드 2, '11'인 경우에는 모드 3이 된다. 상기 암호 모드가 선택되면, 상기 암호 모드에 대응하여 컨텐츠를 해독하고 해독된 컨텐츠에 대한 AV스트림을 출력한다(S558).

<27> 도 6은 본 발명에 따른 3가지 유형의 2-bit 값을 내장하고 있는 데이터 해독을 위한 장치의 구성을 나타내는 예시도로서, 데이터 해독 장치(S600)는 AV스트림(610)을 수신하고, CCI코드 검사부(620)에서 상기 수신한 AV 스트림에서 CCI코드값을 검사한다. 만일 CCI코드값이 '00'인 경우에는 해독모듈(630)을 거치지 않고 바로 AV스트림 출력부(640)를 통하여 출력하게 된다. 반면에 CCI코드값이 '01', '10', '11'인 경우에 해독모듈(630)에서는 상기 CCI코드값과 동일한 값을 컨텐츠를 해독하기 위한 key 값의 최상위비트(MSB) 또는 최하위비트(LSB)에 삽입한다. 만일 불법으로 CCI코드값이 변경되었다면, 컨텐츠를 암호화하는데 사용된 킷값과 다른 킷값이 생성됨으로써 컨텐츠의 해독이 불가능하게 된다. 상기와 같은 방법으로 해독된 AV스트림은 AV스트림 출력부(640)를 통하여 출력하게 된다.

<28> 도 7은 본 발명에 따른 보다 구체적인 실시예로서, 3종류의 DES(Data Encryption Standard) 암호를 이용한 데이터 해독을 위한 장치의 구성을 나타내는 예시도이다. DES암호는 암호키와 복호키가 같은 대칭키 암호로 1960년대 말에 IBM에서 개발하여 1977년 미국 표준 암호 알고리즘

으로 채택되어 속도가 빠르기 때문에 금융기관 등 여러 분야에서 세계적으로 사용되고 있는 암호이다. DES암호는 대칭 블록암호로서 평문의 각 블록의 길이가 64비트이고 키가 64비트(실제로는 56비트가 키이고 8비트는 검사용)이며 암호문이 64비트인 암호이다. DES 알고리즘은 64비트의 평문이 16라운드의 Feistel 연산을 거쳐 64비트의 암호문이 나오게 하는 것이다.

<29> 2중 DES(Double_DES)는 56비트인 2개의 서로 다른 암호키 112비트를 사용하여 DES를 2번 중복하여 실행하는 알고리즘이고, 3중 DES(Triple_DES)는 56비트인 2개의 서로 다른 암호키 112비트를 사용하여 DES를 3번 중복하여 실행하는 알고리즘이다.

<30> 본 발명에 있어서는 해독모듈(730)이 CCI값이 '01'인 경우에는 DES해독 모듈(731)을 수행하고, CCI값이 '10'인 경우에는 2중 DES(Double_DES)해독 모듈(732)을 수행하고, CCI값이 '11'인 경우에는 3중 DES(Triple_DES)해독 모듈(733)을 수행한다. 상기 각각의 모듈(731, 732, 733)에 사용하는 킷값은 암호화할 때의 킷값과 동일한 값을 사용한다.

<31> 지금까지 설명한 CCI코드값에 따른 제어모드를 다르게 구현하는 방법 외에도 암호화/해독 프로세스를 변경하는 방법(보안 등급의 다양화, high, medium, low), 복사가 불가능한 영역에 CCI코드값을 삽입하여 CCI값을 비교하여 다를 경우 더 이상 실행하지 않거나 해당하는 CCI 값을 컨텐츠를 암호화/해독하는데 사요되는 키의 입력 데이터로 활용하는 방법 등도 고려할 수 있다.

<32> 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 한정하는 것은 아니다.

【발명의 효과】

<33> 상기한 바와 같이 이루어진 본 발명에 따르면, 제3자에 의한 데이터 불법 복제를 더욱 효과적으로 방지할 수 있고, 데이터의 중요도에 따른 데이터의 보다 안정적으로 데이터를 보호할 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

데이터의 복제방지를 위한 제어정보를 설정하는 제어정보 설정부;

상기 설정된 제어정보에 따른 각각의 제어모드에 따라 상기 데이터를 상기 제어모드에 따른 별개의 방법으로 암호화하는 데이터 암호화부;

상기 데이터 암호화부에서 제공하는 데이터를 전송하는 데이터 전송부를 포함하는 데이터 복제방지를 위한 전송장치.

【청구항 2】

계층별 암호화된 데이터를 수신하는 데이터 수신부;

상기 수신된 데이터로부터 데이터의 복제방지를 위한 제어정보를 추출하는 제어정보 추출부;

상기 추출된 제어정보에 따른 각각의 제어모드에 대응하여 상기 제어모드에 따른 별개의 방법으로 데이터를 해독하는 데이터 해독부를 포함하는 데이터 복제방지를 위한 수신장치.

【청구항 3】

제1항 또는 제2항에 있어서,

상기 제어정보는 카피제어정보(Copy Control Information, CCI)를 포함하는 데이터 복제방지를 위한 장치.

【청구항 4】

제1항 또는 제2항에 있어서,

상기 제어모드는 절대로 카피할 수 없는 제1모드, 1회만 카피할 수 있고, 카피한 후에는 절대로 카피할 수 없는 제2모드, 카피할 수 있으나 데이터가 암호화된 제3모드를 포함하는 데이터 복제방지를 위한 장치.

【청구항 5】

제2항에 있어서,

상기 수신장치는 AV스트림 정보를 사용자에게 제공하는 미디어 재생장치를 포함하는 데이터 복제방지를 위한 장치.

【청구항 6】

데이터의 복제방지를 위한 제어정보를 설정하고, 상기 설정된 제어정보에 따른 각각의 제어모드에 따라 상기 데이터를 상기 제어모드에 따른 별개의 방법으로 암호화하고, 상기 암호화된 데이터를 전송하는 전송장치와;

상기 전송된 데이터를 수신하여 상기 제어정보를 추출하고, 상기 추출된 제어정보에 따른 각각의 제어모드에 대응하여 상기 제어모드에 따른 별개의 방법으로 데이터를 해독하는 수신장치를 포함하는 데이터 복제방지를 위한 시스템.

【청구항 7】

제6항에 있어서,

상기 제어정보는 카피제어정보(Copy Control Information, CCI)를 포함하는 데이터 복제방지를 위한 시스템.

【청구항 8】

제6항에 있어서,

상기 제어모드는 절대로 카피할 수 없는 제1모드, 1회만 카피할 수 있고, 카피한 후에는 절대로 카피할 수 없는 제2모드, 카피할 수 있으나 데이터가 암호화된 제3모드를 포함하는 데이터 복제방지를 위한 시스템.

【청구항 9】

제6항에 있어서,

상기 수신장치는 AV스트림 정보를 사용자에게 제공하는 미디어 재생장치를 포함하는 데이터 복제방지를 위한 시스템.

【청구항 10】

복제방지를 위한 제어정보를 설정하고, 상기 설정된 제어정보에 따른 각각의 제어모드에 대응하여 상기 제어모드에 따른 별개의 방법으로 데이터를 암호화하여 전송하는 제1단계;

상기 전송된 데이터를 수신하고, 상기 수신한 데이터로부터 상기 제어정보를 추출하는 제2단계;

상기 추출된 제어정보에 따른 각각의 제어모드에 대응하여 상기 제어모드에 따른 별개의 방법으로 데이터를 해독하는 제3단계를 포함하는 데이터 복제방지 방법

【청구항 11】

제10항에 있어서,

상기 제어정보는 카피제어정보(Copy Control Information, CCI)를 포함하는 데이터 복제방지 방법.

【청구항 12】

제10항에 있어서,

상기 제어모드는 절대로 카피할 수 없는 제1모드, 1회만 카피할 수 있고, 카피한 후에는 절대로 카피할 수 없는 제2모드, 카피할 수 있으나 데이터가 암호화된 제3모드를 포함하는 데이터 복제방지 방법.

【청구항 13】

제10항에 있어서,

상기 수신장치는 AV스트림 정보를 사용자에게 제공하는 미디어 재생장치를 포함하는 데이터 복제방지 방법.

【청구항 14】

복제방지를 위한 제어정보를 포함하고, 상기 제어정보에 따른 각각의 제어모드에 따라 상기 제어모드에 따른 별개의 방법으로 암호화된 데이터를 기록한 기록매체.

【청구항 15】

제14항에 있어서,

상기 제어정보는 카피제어정보(Copy Control Information, CCI)를 포함하는 기록매체.

【청구항 16】

제14항에 있어서,

상기 제어모드는 절대로 카피할 수 없는 제1모드, 1회만 카피할 수 있고, 카피한 후에는 절대로 카피할 수 없는 제2모드, 카피할 수 있으나 데이터가 암호화된 제3모드를 포함하는 기록매체.

【도면】

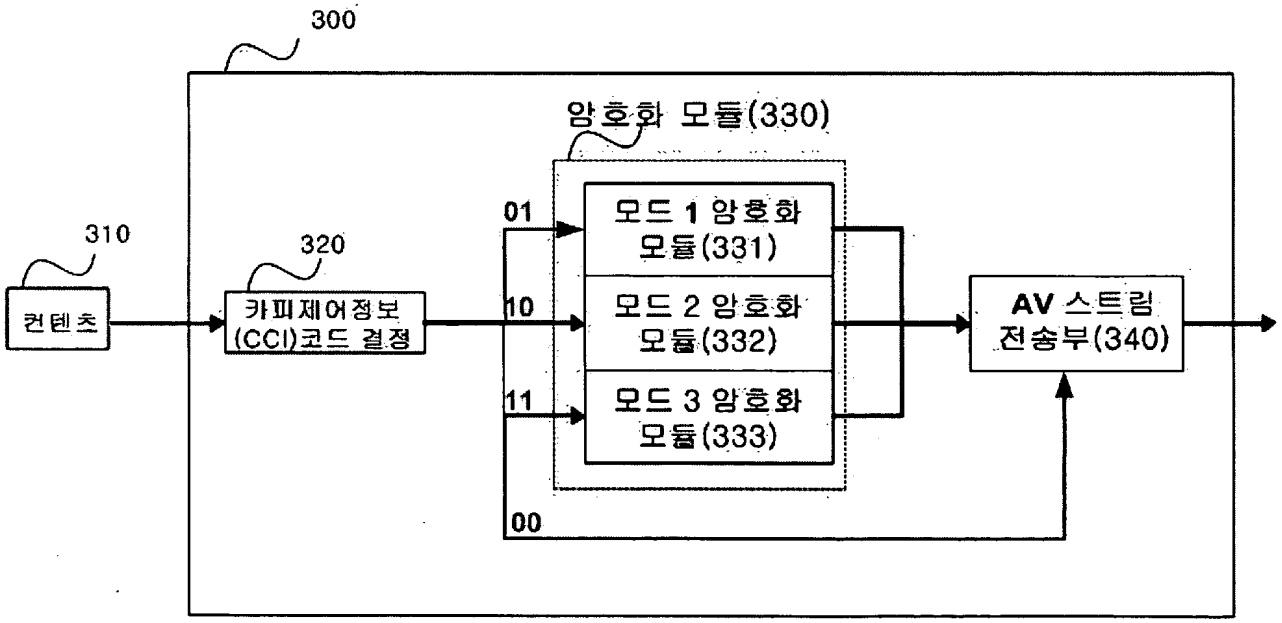
【도 1】

AV 스트림의 CCI 코드 및 상태(status)		암호 상태(Status)
00	Copy free	비암호화
01	Copy free but encrypted	암호화
10	Copy one generation	암호화
11	No more copy or copy never	암호화

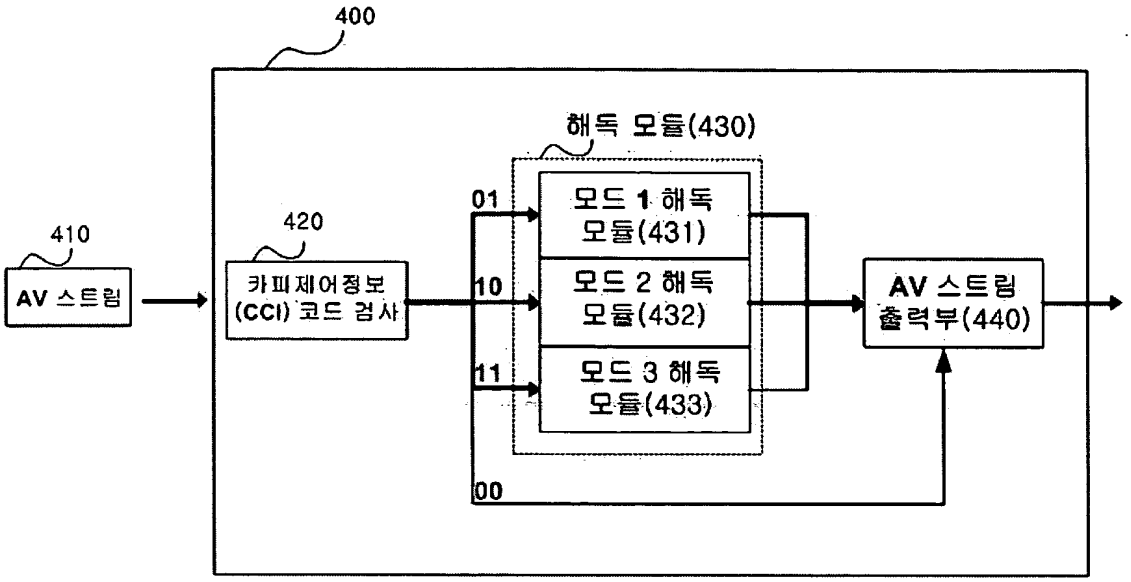
【도 2】

AV 스트림의 CCI 코드 및 상태(status)		암호 상태(Status)	암호/해독 모드
00	Copy free	비암호화	-
01	Copy free but encrypted	암호화	모드 1
10	Copy one generation	암호화	모드 2
11	No more copy or copy never	암호화	모드 3

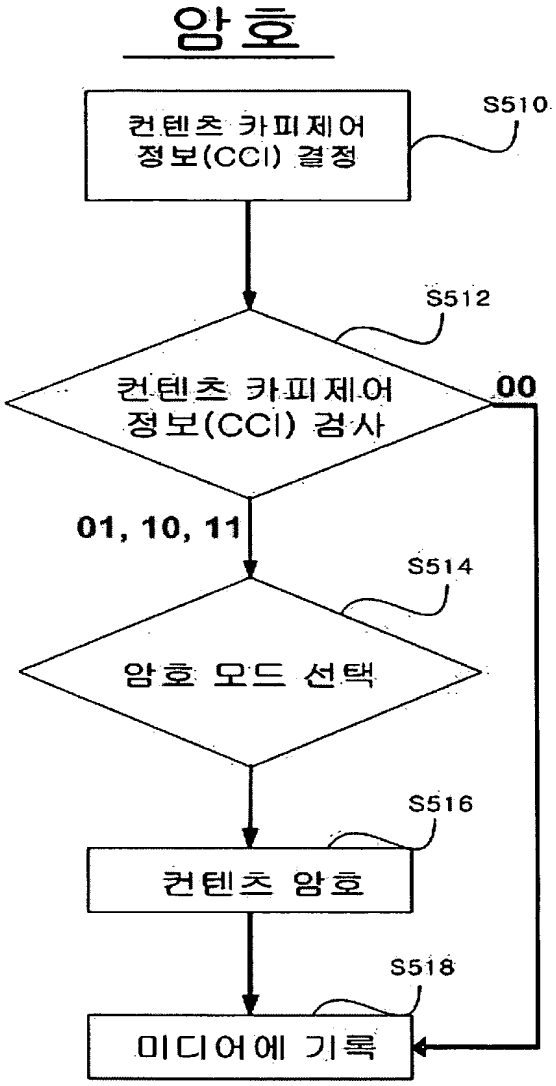
【도 3】



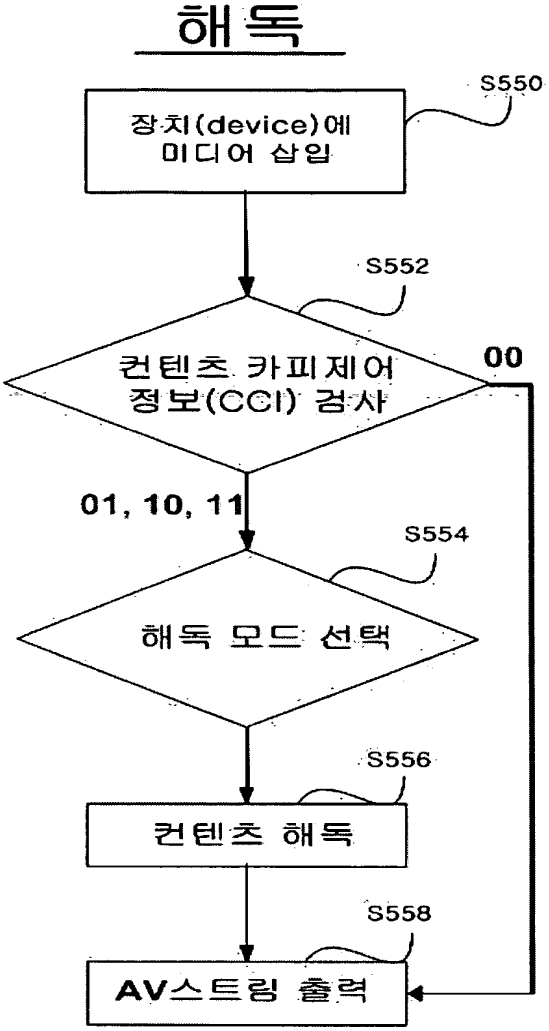
【도 4】


400
해독 모듈(430)
410
AV 스트림
420
카피제어정보 (CCI) 코드 검사
01
10
11
00
모드 1 해독 모듈(431)
모드 2 해독 모듈(432)
모드 3 해독 모듈(433)
AV 스트림 출력부(440)

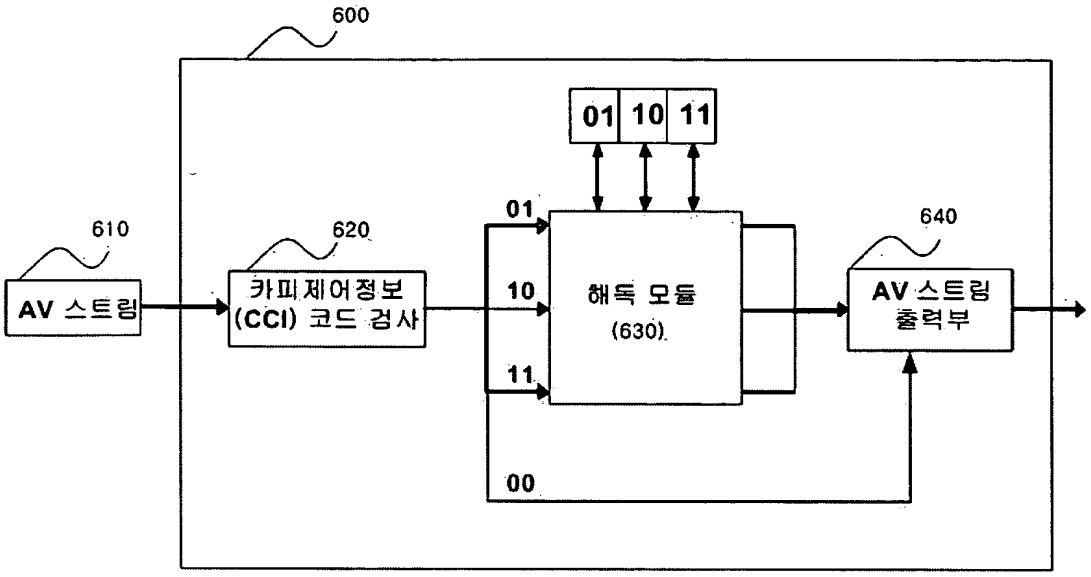
【도 5a】


암호
S510
컨텐츠 카피제어 정보(CCI) 결정
S512
컨텐츠 카피제어 정보(CCI) 검사
00
01, 10, 11
S514
암호 모드 선택
S516
컨텐츠 암호
S518
미디어에 기록

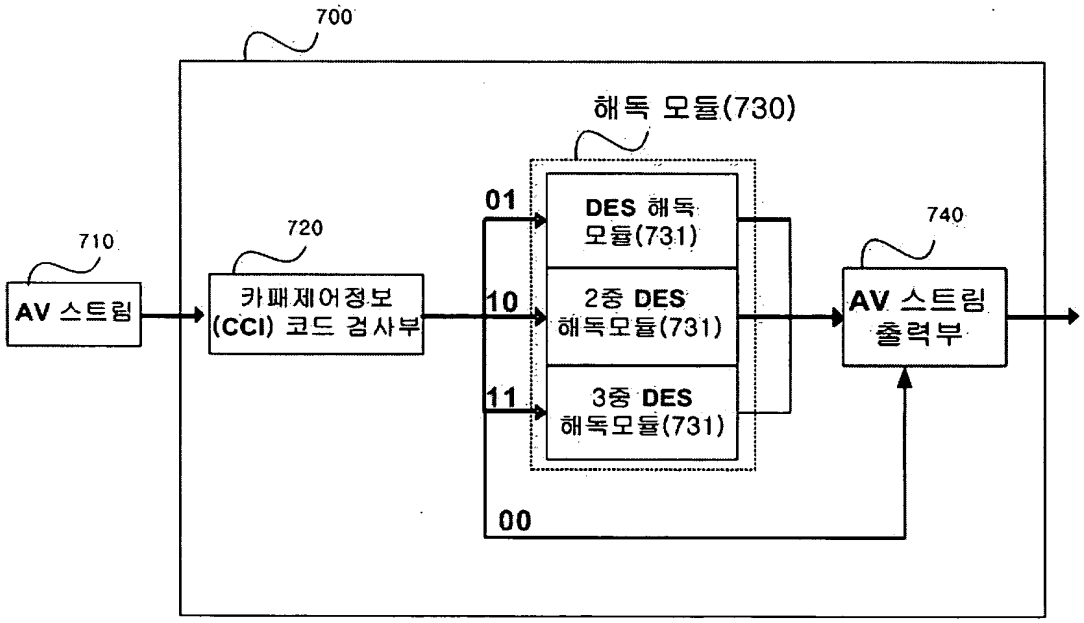
【도 5b】


해독
S550
장치(device)에 미디어 삽입
S552
컨텐츠 카피제어 정보(CCI) 검사
00
01, 10, 11
S554
해독 모드 선택
S556
컨텐츠 해독
S558
AV스트림 출력

【도 6】


600
01
10
11
610
620
640
AV 스트림
카피제어정보
(CCI) 코드 검사
01
10
11
00
해독 모듈
(630)
AV 스트림
출력부

【도 7】


700
해독 모듈(730)
710
720
740
AV 스트림
카패제어정보
(CCI) 코드 검사부
01
10
11
00
DES 해독
모듈(731)
2중 DES
해독모듈(731)
3중 DES
해독모듈(731)
AV 스트림
출력부